IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Patent Application of

Andrew M. Spencer

Application No. 10/689,157

Filed: October 20, 2003

For: Removable Information Storage Device that Includes a Master Encryption Key and Encryption Keys

Group Art Unit: 2438

Examiner: Truong, Thanhnga B.

Confirmation No.: 9457

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Following Appellant's filing of an Appeal Brief on 13 January 2009, prosecution of this application was reopened by the Examiner with a non-final Office Action dated 29 April, 2009. The Examiner subsequently issued a final Office Action dated 27 November 2009 (the "Office Action" or the "Action"). Having reviewed the final Office Action of 27 November 2009, Appellant hereby requests re-instatement of the appeal in this application and file the present updated Appeal Brief in support of the re-instated appeal. Each of the topics required by Rule 41.37 is presented herewith and is labeled appropriately.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive W., Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no appeals or interferences related to the present application of which the Appellant is aware.

III. Status of Claims

No claims have been cancelled.

Claims 16-26 have been withdrawn from consideration under the imposition of a previous Restriction Requirement.

Claims 1-15 and 28-29 are pending in the application and stand finally rejected.

Claims 27 and 30 are pending in the application and stand neither rejected nor allowed. Claims 27 and 30 have not been withdrawn from consideration.

Accordingly, Appellant appeals from the final rejection of claims 1-15 and 28-29, which claims are presented in the Appendix.

IV. Status of Amendments

No amendments have been filed subsequent to the Office Action of November 27, 2009, from which Appellant takes this appeal.

V. Summary of Claimed Subject Matter

A summary of the subject matter defined in each of the independent claims involved in the present appeal is given below in accordance with the requirements of 35 C.F.R. § 41.37(c)(1)(v).

The claimed subject matter discloses apparatus and methods for encrypting and decrypting information in a removable information storage device (14) suitable for use with a host (12). (*E.g.*, Appellant's Specification, p. 2 lines 5-12, p. 3 line 20 to p. 4 line 14, Fig. 1). The removable information storage device (14) includes a non-volatile memory (46) configured to store a master encryption key (*e.g.*, Appellant's Specification, p. 5 lines 11-15, p. 21 lines 8-11, p. 22 lines 1-3, Figs. 1 and 12-13) and a non-volatile magnetic memory (18) configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 line 6 to p. 22 line 30, Figs. 1 and 12-13).

Turning to Appellant's specific independent claims,

Claim 1 recites:

A removable information storage device (14) suitable for use with a host (12) (*e.g.*, Appellant's Specification, p. 2 lines 5-12, p. 3 line 20 to p. 4 line 14, Fig. 1), comprising:

a non-volatile memory (46) configured to store a master encryption key (*e.g.*, Appellant's Specification, p. 5 lines 11-15, p. 21 lines 8-11, p. 22 lines 1-3, Figs. 1 and 12-13); and

a non-volatile magnetic memory (18) configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted

using the encryption keys (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 line 6 to p. 22 line 30, Figs. 1 and 12-13).

Claim 27 recites:

A method of encrypting encryption keys using a master encryption key in an information storage device (14) (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 line 6 to p. 22 line 30, Figs. 1 and 12-13), comprising:

providing encryption keys to the information storage device (14) (*e.g.*, Appellant's Specification, p. 3 line 20 to p. 4 line 14, p. 4 lines 29-32, p. 21 lines 4-8 and 31-32, Figs. 1 and 12-13);

reading a master encryption key from a non-volatile memory (46) (*e.g.*, Appellant's Specification, p. 5 lines 11-15, p. 21 lines 8-11, p. 22 lines 1-3, Figs. 1 and 12-13);

encrypting each one of the encryption keys using the master encryption key (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 lines 6-28, Figs. 1 and 12-13); and

writing the encrypted encryption keys to a random access memory (18) (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 line 6 to p. 22 line 30, Figs. 1 and 12-13).

Claim 28 recites:

A method of decrypting encryption keys in an information storage device (14) (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 line 6 to p. 22 line 30, Figs. 1 and 12-13), comprising:

reading encrypted encryption keys from a magnetic random access memory (18) (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 21 line 31 to p. 22 line 1, Figs. 1 and 12-13);

reading a master encryption key from a first non-volatile memory (46) (*e.g.*, Appellant's Specification, p. 5 lines 11-15, p. 21 lines 8-11, p. 22 lines 1-3, Figs. 1 and 12-13); and

decrypting each one of the encryption keys using the master encryption key (*e.g.*, Appellant's specification, p. 4 line 29 to p. 5 line 10, p. 6 line 10 to p. 8 line 9, p. 8 line 20 to p. 10 line 5, p. 22 lines 1-30, Figs. 1 and 12-13).

VI. Grounds of Rejection to be Reviewed on Appeal

The Office Action raised the following grounds of rejection.

(1) Claim 1 was rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,159,182 to Eisele ("Eisele").

(2) Claims 2-15 and 28-29 were rejected under 35 U.S.C. § 102(b) as anticipated by Eisele, or in the alternative, under 35 U.S.C. § 103(a) as being obvious over Eisele.

According, Appellant hereby requests review of each of the above grounds of rejection in the present appeal.

VII. Argument

(1) Claim 1 is patentable over Eisele:

Claim 1 was rejected under 35 U.S.C. § 102(b) as being anticipated by Eisele. For at least the following reasons, this rejection should not be sustained.

Claim 1:

Claim 1 recites:

> A removable information storage device suitable for use with a host, comprising:
> a non-volatile memory *configured to store a master encryption key*; and
> a non-volatile magnetic memory *configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys*.

(Emphasis added).

Appellant notes that "[t]he examiner bears the initial burden . . . of presenting a *prima facie* case of unpatentability." *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In a rejection made under § 102, this burden is substantial, as a *prima facie* case of anticipation requires a demonstration that "*each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987) (emphasis added). *See* M.P.E.P. § 2131.

In 2008, the Court of Appeals for the Federal Circuit further clarified that "unless a reference discloses within the four corners of the document *not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim*, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102." *Net MoneyIN, Inc. v. Verisign, Inc.*, 545 F.3d 1359, 1371, 88 U.S.P.Q.2d 1751, 1759 (Fed. Cir. 2008) (emphasis added).

In light of these considerations, the recent Office Action does not meet the requisite burden to establish a *prima facie* case of anticipation against claim 1, as the Action has failed to demonstrate that Eisele teaches or suggests "each and every element" recited in claim 1. Specifically, Eisele does not teach or suggest a storage device having "a non-volatile magnetic memory configured to store encryption keys which have been encrypted using [a] master encryption key," where the "master encryption key" is stored on a separate "non-volatile memory" of the storage device. (Claim 1).

Eisele is directed to a storage device that includes both a floppy disk-type magnetic memory medium (7) and an integrated circuit (2) that interacts with non-magnetic, nonvolatile storage memory (9). (*E.g.*, Eisele, col. 4 lines 6, 40; col. 5 lines 20-24; Figs. 2, 3, 8). As noted by the Action, Eisele teaches that either or both of the magnetic memory medium (7) and the non-magnetic, nonvolatile storage memory (9) can store "one or more cryptographic algorithms, secret codes etc. in such a way that they cannot be reproduced." (Eisele, col. 5 lines 20-30; *see* Action, p. 5).

The Examiner asserts that these teachings in Eisele anticipate the "non-volatile memory configured to store a master encryption key" and the "non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys" recited in claim 1. Appellant respectfully disagrees, for at least the reason that to demonstrate anticipation, the allegedly identical invention "must be shown in as complete detail as is contained in the . . . claim." M.P.E.P. § 2131 (citing to *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)). Neither Eisele itself nor the Examiner's characterization of Eisele shows the subject matter recited in claim 1 "in as complete detail as is contained in the claim," *Richardson*, 868 F.2d at 1236, 9 USPQ2d at 1920, particularly

with regard to the different types of encryption keys and separate storage of encryption keys by type, as recited in claim 1.

In the present case, the Action has merely demonstrated that Eisele teaches a magnetic non-volatile storage medium and a non-magnetic non-volatile storage medium, where both of the media may be used to store "one or more cryptographic algorithms, secret codes, etc. in such a way that they cannot be reproduced." (Eisele, col. 5 lines 20-24). As such, the Action has failed to demonstrate that Eisele teaches or suggests the existence of a "master encryption key" and other "encryption keys," where the master encryption key is used to encrypt the other encryption keys. (Claim 1). Indeed, the Action is unable to demonstrate this teaching in Eisele for the simple reason that Eisele does not teach or suggest the use of different types of encryption keys, or that one type of encryption key is used to encrypt encryption keys of a different type. (*See id.*).

Even if, *arguendo*, Eisele did teach or suggest the "master encryption key" and other "encryption keys" recited in claim 1, where the master encryption key is used to encrypt the other encryption keys, the Action has still failed to demonstrate that Eisele teaches storing the master encryption key on one of the storage media and the other encryption keys on the other of the storage media. Again, the Office cannot make such a demonstration, as Eisele makes no teaching or suggestion separating encryption keys by type to different storage media in the same device. Regarding this subject matter, the Examiner cites to Eisele's teaching that portions of a program may be divided between a host Electronic Data Processing (EDP) computer and the processor in a removable data storage device. (Action, p. 3) (citing to Eisele, col. 5 lines 20-24). The Action maintains the position that because Eisele discloses a need to "load the element's memory units with one or more cryptographic algorithms, secret codes etc. . . . in such a way that they cannot be reproduced, . . . Eisele precisely teaches the

use of the two different memories to store encryption keys." (*Id.*). Appellant respectfully disagrees. Eisele here simply teaches that portions of a program may be executed by a host device and a removable storage device, not that different types of encryption keys are divided between different types of data storage **in the same removable storage device** as in claim 1.

Even if, *arguendo*, Eisele taught dividing the portions of a program between different storage media in the same removable storage device, the Examiner has still failed to demonstrate that Eisele teaches the use of two different memories in a single removable storage device to separately store different types of **encryption keys**. Furthermore, even if the Examiner were correct in its assertion that "the use of two different memories to store encryption keys" prevents cryptographic algorithms and secret codes from being reproduced, (Action, p. 4), for Eisele to anticipate the separate storage of different types of encryption keys recited in claim 28, the Examiner must demonstrate that the separate storage of different types of encryption keys recited in claim 28 is the ***only*** way to prevent reproduction of codes or algorithms as disclosed by Eisele. *See In re Robertson*, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) ("Inherency, however, ***may not be established by probabilities or possibilities***. The mere fact that a certain thing may result from a given set of circumstances is not sufficient."); *Ex parte Levy*, 17 USPQ2d 1461, 1464 (BPAI 1990) ("[T]he examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic *necessarily* flows from the teachings of the applied prior art.") (emphasis in original); M.P.E.P. § 2112 (quoting *Levy*). Undoubtedly the separate storage of different types of encryption keys as recited in claim 28 is not the **only** way to prevent reproduction of codes or algorithms, and therefore this subject matter in claim 28 does not *necessarily* flow from the teachings of Eisele. *Levy*, 17 USPQ2d at 1464.

Because Eisele fails to teach or suggest a "master encryption key" that is used to encrypt other encryption keys, and because Eisele also fails to teach or suggest separating the encryption keys by type to different storage media in the same device, Eisele *cannot* teach or suggest "a non-volatile memory configured to store a master encryption key" and "a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys." (Claim 1).

Again, "[a] claim is anticipated [under 35 U.S.C. § 102] only if *each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal*, 814 F.2d at 631, 2 U.S.P.Q.2d at 1053. *See Verisign*, 545 F.3d at 1371, 88 U.S.P.Q.2d at 1759; M.P.E.P. § 2131. Thus, Eisele cannot anticipate claim 1 because, for the above reasons, Eisele fails to teach or suggest all of the subject matter present in claim 1. Given that the Office has not met its burden to demonstrate the *prima facie* unpatentability of claim 1, the rejection of claim 1 and its dependent claims based on Eisele should not be sustained.

(2) Claims 2-15 and 28-29 are patentable over Eisele:

Claims 2-15 and 28-29 were rejected under 35 U.S.C. § 102(b) as being anticipated by Eisele, and in the alternative, under 35 U.S.C. § 103(a) as being obvious over Eisele. For at least the following reasons, these alternate rejections should not be sustained.

Claim 2:

The rejection of claim 2 should not be sustained for at least the same reasons given above in favor of the patentability of independent claim 1.

Additionally, claim 2 recites "an encryption and decryption engine configured to encrypt and decrypt the encryption keys using the master encryption key." In response, the Action cites to Eisele's teaching that data stored on a disk drive may be encrypted, and that the data may be decrypted when provided to an authorized user. (Action, p. 7) (citing to Eisele, col. 5 lines 12-19). As demonstrated above, these teachings are insufficient to demonstrate that Eisele teaches, suggests, or otherwise renders obvious the encryption and decryption of **encryption keys** using a master encryption key where the **encryption keys encrypted by the master encryption key** are used to encrypt data. This subject matter is plainly not present in Eisele. Consequently, the Action has failed to demonstrate the *prima facie* anticipation or obviousness of claim 2. For at least these additional reasons, the rejection of claim 2 should not be sustained.

Claim 10:

The rejection of claim 10 should not be sustained for at least the same reasons given above in favor of the patentability of independent claim 1.

Additionally, claim 10 recites "wherein the non-volatile magnetic memory is a magnetic random access memory." In this regard, the Action asserts that Eisele's teaching of a magnetic disk storage medium anticipates or renders obvious this subject matter. (Action, p. 8) (citing to Eisele, col. 4 lines 18-28, col. 5 lines 20-24, Fig. 3). It is well-known in the art that a magnetic disk (7) is not random access memory ("RAM"), as the mechanical movement of a read/write head for a magnetic disk does not allow for uniform read/write times on the disk irrespective of address. (*See, e.g.*, RAM – Definition and More from the Free Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/RAM (last accessed March 2, 2010) (defining random access memory as "computer memory on which

data can be both read and written and on which the location of data does not affect the speed of its retrieval"). Eisele does not teach or suggest a magnetic RAM anywhere, and does not support the Examiner's position.

As such, the Action has failed to demonstrate the *prima facie* anticipation or obviousness of claim 10 with regard to Eisele. Consequently, the rejection of claim 10 should not be sustained for at least these additional reasons.

Claims 11-13:

The rejection of claims 11-13 should not be sustained for at least the same reasons given above in favor of the patentability of independent claim 1.

Additionally, claim 11 recites "wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas." Claim 12 recites "wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys and the encrypted data are stored in the first areas." Claim 13 recites "wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas."

With respect to each of claims 11-13, the Action merely cites again to the portion of Eisele which teaches that data can be encrypted on a removable storage device and that different portions of a program may be executed by a host device and a processor in a removable storage device. (Action, p. 8) (citing to Eisele, col. 5 lines 20-30). It will be readily apparent that this portion of Eisele makes no teaching or suggestion of partitioning a

memory or of the allocation of encrypted keys and other encrypted data between the partitions. Again, the Action is extracting teachings from Eisele that are plainly not there.

As such, the Action has failed to meet its burden of demonstrating the *prima facie* anticipation or obviousness of claims 11-13 with regard to Eisele. Consequently, the rejection of claims 11-13 should not be sustained for at least these additional reasons.

Claims 14-15:

The rejection of claims 14-15 should not be sustained for at least the same reasons given above in favor of the patentability of independent claim 1 and dependent claim 13.

Additionally, claim 14 recites "wherein the first areas are located at one or more predetermined address locations within the second non-volatile memory." Claim 15 recites "wherein the first areas are located at one or more random address locations within the second non-volatile memory." In this regard, the Action merely cites to the same portion of Eisele which teaches that data can be encrypted on a removable storage device and that different portions of a program may be executed by a host device and a processor in a removable storage device. (Action, p. 8) (citing to Eisele, col. 5 lines 20-30). It will be readily apparent from a careful reading of this portion of Eisele that the Action has failed to identify any teaching in Eisele concerning the address locations of the "first areas" recited in claim 13.

As such, the Action has failed to meet its burden of demonstrating the *prima facie* anticipation or obviousness of claims 14-15 with regard to Eisele. Consequently, the rejection of claims 14-15 should not be sustained for at least these additional reasons.

Claim 28:

Claim 28 recites:

> A method of decrypting encryption keys in an information storage device, comprising:
> reading *encrypted encryption keys* from *a magnetic random access memory*;
> reading *a master encryption key* from a first non-volatile memory; and
> *decrypting each one of the encryption keys using the master encryption key*.

(Emphasis added).

A. Anticipation Under 35 U.S.C. § 102(b)

Eisele also fails to anticipate the method of claim 28. Specifically, as demonstrated above with respect to independent claim 1, Eisele does not teach or suggest the use of separate types of encryption keys, namely "a master encryption key" and other "encryption keys." (Claim 28). As additionally demonstrated above with respect to claim 1, Eisele fails to teach or suggest the storing the master encryption key in one storage medium ("a first non-volatile memory") and the other encryption keys in another storage medium ("a magnetic random access memory"). (*Id.*). As further demonstrated above with respect to claim 1, Eisele does not teach the encryption of encryption keys using the master encryption key, and therefore cannot teach or suggest "decrypting each one of the encryption keys using the master encryption key." (*Id.*).

The Action asserts that Eisele teaches "decrypting each one of the encryption keys using the master encryption key" because Eisele teaches the verification of authorized data access in a processor of the magnetic disk (7) through a PIN code entered by a user, and because Eisele teaches that the processor of the magnetic disk (7) can encrypt and decrypt data stored thereon. (Action, p. 4) (citing to Eisele, col. 4 line 60 to col. 5 line 8, col. 5 lines 12-16). Appellant respectfully disagrees. The ability of the devices in Eisele to encrypt and decrypt general data stored on the magnetic disk is insufficient to establish that Eisele teaches

the encryption of **encryption keys through the use of a master encryption key**. (Claim 28). Nowhere does Eisele teach or suggest that a PIN code or anything else acts as a master encryption key to encrypt other encryption keys. By asserting otherwise, the Examiner is unfairly reading subject matter from Eisele that is completely outside the scope of Eisele.

Furthermore, the Action incorrectly asserts that the magnetic disk (7) of Eisele teaches the "magnetic random access memory" recited in claim 28. (Action, pp. 5-6) (citing to Eisele, Figs. 2-3, 5-6, and col. 5 lines 5-9 and 12-19). Appellant respectfully disagrees. Again, it is well-known in the art that a magnetic disk (7) is not random access memory ("RAM"), as the mechanical movement of a read/write head for a magnetic disk does not allow for uniform read/write times on the disk irrespective of address. (*See, e.g.*, RAM – Definition and More from the Free Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/RAM (last accessed March 2, 2010) (defining random access memory as "computer memory on which data can be both read and written and on which the location of data does not affect the speed of its retrieval"). Eisele does not teach or suggest a magnetic RAM anywhere, and by asserting otherwise, the Action is again unfairly extracting teachings from Eisele that simply do not exist.

Again, "[a] claim is anticipated [under 35 U.S.C. § 102] only if *each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal*, 814 F.2d at 631, 2 U.S.P.Q.2d at 1053. *See Verisign*, 545 F.3d at 1371, 88 U.S.P.Q.2d at 1759; M.P.E.P. § 2131. Thus, Eisele cannot anticipate claim 28 because, for the above reasons, Eisele fails to teach or suggest all of the subject matter present in claim 28. Because the Office has not met its burden to demonstrate *prima facie* unpatentability of claim 28, the rejection of claim 28 and its dependent claims based on Eisele should not be sustained.

B. Obviousness Under 35 U.S.C. § 103(a)

The Action also fails to meet its burden to establish a *prima facie* case of obviousness against claim 28, which requires a showing that all of the subject matter in claim 28 would be obvious to one having ordinary skill in the art based on the teachings of Eisele. *See* M.P.E.P. § 2143. As amply demonstrated above, Eisele fails to teach or suggest various elements recited in claim 28, specifically (a) separate types of encryption keys, namely "a master encryption key" and other "encryption keys;" (b) the storage of the master encryption key in a separate storage medium ("a first non-volatile memory") from the other encryption keys ("a magnetic random access memory"); (c) "decrypting each one of the encryption keys using the master encryption key;" and (d) a "magnetic random-access memory." (Claim 28).

For claim 28 to be obvious over Eisele alone, the Office bears the burden of demonstrating that the differences between Eisele and claim 28 would be obvious to one having ordinary skill in the art. In this regard, the Action does not demonstrate that (a) the use of separate types of encryption keys, (b) the separate storage of encryption keys by type, and (c) the encryption of encryption keys with a "master encryption key" would have been known to one having ordinary skill in the art at the time of the invention or that one having ordinary skill in the art would have sufficient motivation to adapt the device of Eisele to include any of these features. *See* M.P.E.P. § 2143. As such, the Action has failed to demonstrate the *prima facie* obviousness of these features.

With respect to the "magnetic random access memory" recited in claim 28, the Action asserts that "Eisele implies that the magnetic disk includes read/write heads 16 and 17, wherein MRAM uses the same read/write functionality as in disk 7 of Eisele" and that it would have been obvious to "have modified the invention of Eisele to clearly disclose disk 7

as being a magnetic random access memory." (Action, p. 6). Appellant respectfully disagrees. It will be readily apparent to those having skill in the art that magnetic random access memory does not use a mechanically movable read/write head like that of the disk in Eisele to perform read/write functions. (*See, e.g.*, Appellant's specification, Figs. 2-4) (describing architecture and read/write operations of exemplary magnetic read-only memory cells). By contrast, magnetic random access memory employs a system of row and column select lines to individually impart a read/write magnetic signal to individual storage elements. (*See id.*).

It would not have been obvious to one having ordinary skill in the art to replace the disk 7 of Eisele with a magnetic random access memory module for at least the reason that a disk does not interface with a host device in the same way that a RAM module does. Specifically, unlike disk 7 of Eisele, a RAM module cannot be placed into a magnetic disk drive and read with a magnetic read/write head. Furthermore, Eisele is directed to a portable nonvolatile disk that can store data without a power supply, whereas RAM is volatile memory that is not amenable to portability, as it requires power to preserve data. Thus, a substitution of a RAM module for magnetic disk 7 of Eisele would render the device of Eisele inoperable. *See* M.P.E.P. § 2143.01 (citing to *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)) (no *prima facie* case of obviousness where a proposed modification of the prior art would change the principle of operation of the prior art invention being modified); *Gillette Co. v. S.C. Johnson & Son, Inc.*, 919 F.2d 720 (Fed. Cir. 1990) ("An analysis of obviousness of a claimed combination must include consideration of the results achieved by that combination.").

Under the analysis required by *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966), to support a rejection under 35 U.S.C. § 103, the scope and content of the prior

art must first be determined, followed by an assessment of the differences between the prior art and the claim at issue in view of the ordinary skill in the art. The Supreme Court has recently reaffirmed that the *Graham* factors "continue to define the inquiry that controls" obviousness rejections under § 103. *KSR Int'l v. Teleflex Inc.*, 550 U.S. 398, 407 (2007). In the present case, the scope and content of the prior art, as evidenced by Eisele, did not include the claimed subject matter, particularly (a) the use of separate types of encryption keys, namely "a master encryption key" and other "encryption keys;" (b) the storage of the master encryption key in a separate storage medium ("a first non-volatile memory") from the other encryption keys ("a magnetic random access memory"); (c) "decrypting each one of the encryption keys using the master encryption key;" and (d) a "magnetic random-access memory." (Claim 28).

The differences between the cited prior art and claim 28 are significant because claim 28 provides a comprehensive data encryption solution for removable storage media that is entirely outside the scope of Eisele and the knowledge available to those of ordinary skill in the art at the time of the invention. Thus, the claimed subject matter provides features and advantages not known or available in the cited prior art. Consequently, the cited prior art will not support a rejection of claim 28 under 35 U.S.C. § 103 and *Graham*. For at least these reasons, the rejection of claim 28 and its dependent claims as obvious over Eisele should not be sustained.

(3) Claim 27 is patentable over Eisele:

The Action failed to reject or allow pending independent claim 27. Claim 27 has not been withdrawn from consideration. Appellant respectfully submits that claim 27 is also patentable over the prior art of record.

Specifically, claim 27 recites:

> A method of *encrypting encryption keys using a master encryption key in an information storage device*, comprising:
> providing encryption keys to the information storage device;
> *reading a master encryption key from a non-volatile memory*;
> *encrypting each one of the encryption keys using the master encryption key*; and
> *writing the encrypted encryption keys to a random access memory*.

(Emphasis added).

As amply demonstrated above with respect to at least independent claims 1 and 28, Eisele does not anticipate or render obvious the method of claim 27. Specifically, as demonstrated above, Eisele does not teach or suggest "reading a master encryption key from a non-volatile memory;" "encrypting each one of the encryption keys using the master encryption key;" and "writing the encrypted encryption keys to a random access memory." (Claim 27). Eisele cannot anticipate claim 27 because Eisele fails to teach "each and every element" recited in claim 27. *Verdegaal*, 814 F.2d at 631, 2 U.S.P.Q.2d at 1053. *See Verisign*, 545 F.3d at 1371, 88 U.S.P.Q.2d at 1759; M.P.E.P. § 2131. Moreover, the differences between Eisele and claim 27 are substantial, and are outside the scope of what would have been obvious to one having ordinary skill in the art. *See Graham*, 383 U.S. at 17-18, M.P.E.P. § 2143.

(3) Claim 30 is patentable over Eisele:

The Action failed to reject or allow pending dependent claim 30. Claim 30 has not been withdrawn from consideration. Appellant respectfully submits that claim 30 is also patentable over the prior art of record for at least the same reasons given above in favor of the patentability of independent claim 28.

In view of the foregoing, it is submitted that the final rejection of the pending claims is improper and should not be sustained. Therefore, a reversal of the Rejection of November 27, 2009 is respectfully requested.

Respectfully submitted,

DATE: March 29, 2010

/Steven L. Nichols/
Steven L. Nichols
Registration No. 40,326

Steven L. Nichols, Esq.
Vancott, Bagley, Cornwall & McCarthy
36 South State Street
Suite 1900
Salt Lake City, Utah 84111
(801) 237-0251 (phone)
(801) 237-0866 (fax)

VIII. CLAIMS APPENDIX

1. (original) A removable information storage device suitable for use with a host, comprising:

a non-volatile memory configured to store a master encryption key; and

a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys.

2. (original) The information storage device of claim 1, further comprising an encryption and decryption engine configured to encrypt and decrypt the encryption keys using the master encryption key and to encrypt and decrypt the data using one or more of the encryption keys.

3. (original) The information storage device of claim 1, wherein the first non-volatile memory is a magnetic memory.

4. (original) The information storage device of claim 1, wherein the first non-volatile memory is a read-only memory which includes fuse elements.

5. (original) The information storage device of claim 1, wherein the first non-volatile memory is a nitrided read-only memory.

6. (original) The information storage device of claim 1, wherein the first non-volatile memory is an erasable programmable read-only memory.

7. (original) The information storage device of claim 1, wherein the first non-volatile memory is an electronically erasable programmable read-only memory.

8. (original) The information storage device of claim 1, wherein the first non-volatile memory is a flash erasable programmable read-only memory.

9. (original) The information storage device of claim 1, wherein the first non-volatile memory is a one time programmable read-only memory.

10. (original) The information storage device of claim 1, wherein the non-volatile magnetic memory is a magnetic random access memory.

11. (original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas.

12. (original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys and the encrypted data are stored in the first areas.

13. (original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas.

14. (original) The information storage device of claim 13, wherein the first areas are located at one or more predetermined address locations within the second non-volatile memory.

15. (original) The information storage device of claim 13, wherein the first areas are located at one or more random address locations within the second non-volatile memory.

16. (withdrawn) A portable memory card, comprising:

a non-volatile memory storage device configured to store one or more encrypted encryption keys and encrypted data; and

a card controller system coupled to the memory storage device configured to store and retrieve the encrypted encryption keys and the encrypted data from the memory storage device, wherein the encryption keys are encrypted and decrypted using a master encryption key and the data is encrypted and decrypted using the encryption keys.

17. (withdrawn) The portable memory card of claim 16, wherein the non-volatile memory is a magnetic memory.

18. (withdrawn) The portable memory card of claim 16, wherein the non-volatile memory is an atomic resolution storage memory.

19. (withdrawn) The portable memory card of claim 16, wherein the card controller system includes a non-volatile master key memory configured to store the master encryption key.

20. (withdrawn) The portable memory card of claim 16, wherein the card controller system includes an encryption and decryption engine configured to store one or more encryption algorithms and use the encryption algorithms to encrypt and decrypt the encryption keys using the master encryption key and encrypt and decrypt the data using the encryption keys.

21. (withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas.

22. (withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys and the encrypted data are stored in the first areas.

23. (withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas.

24. (withdrawn) A memory card, comprising:

a non-volatile master key memory configured to store a master encryption key;

an encryption and decryption engine configured to implement one or more symmetrical encryption key algorithms based on the master encryption key and encryption keys;

a memory storage device comprising an atomic resolution storage device including a field emitter, a media and a micromover, the atomic resolution storage device configured to store the encryption keys after the encryption keys are encrypted using the master encryption key and to store data after the data is encrypted using the encryption keys;

a host interface configured to provide a communication interface to a host;

a memory interface configured to provide a communication interface to the memory storage device;

a data path manager configured to manage communication of the data and the encrypted data between the host and the memory storage device; and

a controller processor configured to control the encryption and decryption of the encryption keys using the master encryption key and the encryption and decryption of the data using the encryption keys.

25. (withdrawn) An information storage device, comprising:

a non-volatile memory storage device configured to store one or more encrypted encryption keys and encrypted data; and

controller means configured to store and retrieve the encrypted encryption keys and the encrypted data from the memory storage device and to encrypt and decrypt the encryption

keys using a master encryption key and to encrypt and decrypt the data using the encryption keys.

26. (withdrawn) The information storage device of claim 25, wherein the controller means includes a non-volatile master key memory configured to store the master encryption key.

27. (previously presented) A method of encrypting encryption keys using a master encryption key in an information storage device, comprising:

providing encryption keys to the information storage device;

reading a master encryption key from a non-volatile memory;

encrypting each one of the encryption keys using the master encryption key; and

writing the encrypted encryption keys to a random access memory.

28. (previously presented) A method of decrypting encryption keys in an information storage device, comprising:

reading encrypted encryption keys from a magnetic random access memory;

reading a master encryption key from a first non-volatile memory; and

decrypting each one of the encryption keys using the master encryption key.

29. (original) The method of claim 28, comprising:

reading encrypted data from the magnetic random access memory; and

decrypting the encrypted data using the encryption keys.

30. (original) The method of claim 28, comprising;

encrypting the data using the encryption keys; and

writing the encrypted data to the magnetic random access memory.

IX. Evidence Appendix

None

X. Related Proceedings Appendix

None

XI. Certificate of Service

None